OIPE JC112
JUN 16 2005
TRADEMARK OFFICE

ZFW
AF

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/723,481
Filing Date	November 28, 2000
In re Application of:	David E. MCDYSAN et al.
Group Art Unit	2155
Examiner Name	Bates, K.
Customer No.	25537
Attorney Docket Number	RIC 00 042
Client Docket Number	09710-1232

Total Number of Pages in This Submission: 33

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Response
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Assignment Papers *(for an Application)*
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition Routing Slip (PTO/SB/69) and Accompanying Petition
- ☐ To Convert a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Small Entity Statement
- ☐ Request of Refund
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Additional Enclosure(s) *(please identify below)*:

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	DITTHAVONG & CARLSON, P.C. Phouphanomketh Ditthavong, Reg. No. 44658
Signature	[signature]
Date	June 15, 2005

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Alexandria, VA 22313-1450 on this date:

Type or printed name	Linda V. Wiley		
Signature	[signature]	Date	June 15, 2005

PTO/SB/17 (12-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Effective on 12/8/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2005

☐ Applicant Claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500.00

Complete if Known	
Application Number	09/723,481
Filing Date	November 28, 2000
First Named Inventor	McDysan, et al.
Examiner Name	Bates, K.
Customer No,	25537
Art Unit	2155
Attorney Docket No.	RIC 00 042

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): ____________

[X] Deposit Account Deposit Account Number: 13-2491 Deposit Account Name: MCI, Inc.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

[X] Charge fee(s) indicated below ☐ Charges fee(s) indicated below, **except for the filing fee**

☐ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180

Total Claims		Extra Claims		Fee ($)		Fee Paid ($)
50	- 50 =	0	x	$50.00	=	0

HP = highest number of total claims paid for, if greater than 20

Indep. Claims		Extra Claims		Fee ($)		Fee Paid ($)
3	- 3 or HP =	0	x	$200.00	=	$ 0.00

HP = highest number of independent claims paid for, if greater than 3

Multiple Dependent Claims Fee ($)	Fee Paid ($)
$360.00	

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41 (a)(1)(G) and 37 CFR 1.16(s).

Total Sheets		Extra Sheets		Number of each additional 50 or fraction thereof			Fee ($)		Fee Paid ($)
0	- 100 =	0	/ 50 =	0	(round up to a whole number)	x	$250.00	=	$ 0.00

4. OTHER FEE(S) | **Fees Paid($)**

Non-English Specification, $130 fee (no small entity discount) ________

Other: Appeal Brief filing fee 500.00

SUBMITTED BY

Signature	[signature]	Registration No. (Attorney/Agent)	44658	Telephone	(703) 425-8508
Name (Print/Type)	Phouphanomketh Ditthavong			Date	June 15, 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: David E. MCDYSAN et al.		Conf. No.:	7586
Application No.:	09/723,481	Group Art Unit:	2155
Filed:	November 28, 2000	Examiner:	Bates, K.
Customer No.:	25537		
Attorney Docket:	RIC 00 042		
Client Docket:	09710-1232		

For: PROGRAMMABLE ACCESS DEVICE FOR A DISTRIBUTED NETWORK ACCESS SYSTEM

APPEAL BRIEF

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated April 15, 2005.

I. REAL PARTY IN INTEREST

MCI, Inc. is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

A Notice of Appeal and Appeal Brief have been filed in co-pending related U.S. Patent Application Serial No. 09/723,480 to McDysan et al., filed November 28, 2000, and entitled "Message, Control and Reporting Interface for a Distributed Network Access System."

III. STATUS OF THE CLAIMS

Claims 1-50 are pending in this appeal. No claim is allowed. This appeal is therefore taken from the final rejection of claims 1-50 on November 18, 2004.

IV. STATUS OF AMENDMENTS

No amendment to the claims has been made since the final Office Action dated November 18, 2004.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present claimed invention addresses problems associated with a network access system. More particularly, the present claimed invention relates to an IP-based communication network including a network access system having distributed and separate routing, signaling, service control, filtering, policy control and other functionality from IP forwarding. (*See, e.g.*, specification, p. 1, lines 25-29)

Conventional monolithic router designs have limited flexibility and extensibility. The present claimed invention recognizes that it would be desirable, in view of the rapid growth of Internet traffic, to dynamically provision, configure, and/or reallocate access capacity to IP-based services. Because access capacity is necessarily limited and providing additional access capacity is a major cost component of networks, the enforcement of intelligent admission control policies and provision of differing qualities of service is vital to the efficient utilization of available access capacity. However, conventional edge routers are not capable of classifying a wide variety of traffic types while enforcing policy controls or of responding to dynamic requests for capacity, and this functionality is difficult to incorporate within currently deployed monolithic edge routers. The present claimed invention accordingly recognizes that it would be desirable to

provide the above as well as additional policy control, network monitoring, diagnostic, and security services in commercialized hardware, while permitting these services to be tailored to meet the needs of individual customers and service providers. (*See, e.g.,* specification, p. 3, line 29 - p. 4, line 14)

A distributed network access system architecture including a programmable access device is introduced. The programmable access device includes first and second network interfaces through which packets are communicated with a network, a forwarding table utilized to route packets communicated between the first and second network interfaces, and a packet header filter. (*See, e.g.*, independent claims 1 and 26) The packet header filter identifies messages received at one of the first and second network interfaces on which policy-based services are to be implemented and passes identified messages via a message interface to an external processor for processing. (*See, e.g.,* independent claims 1, 26, and 50, *see, also, e.g.*, claim 19 and specification, p. 41, line 5 - p. 45, line 8, FIGs. 9A-9E; claim 20 and specification, p. 46, line 4 - p. 47, line 29, FIGs. 10A-10C; and specification, p. 48, line 27 - p. 49, line 25, FIGs. 10G-10H) The packet header filter may be capable of filtering packets for service processing based upon protocol information pertaining to protocol layers higher than layer 3. The programmable access device may also include a usage monitor that reports events, such as session activity levels, to the external processor, a policer that polices packets by reference to programmed traffic parameters (*see, e.g.,* independent claim 50), and a scheduler that schedules the transmission of outgoing packets to support multiple quality of service classes.

In addition to the programmable access device, the distributed network access system architecture may include an external processor and an access router. Thus, conventional, proprietary edge routers are replaced with a distributed network access system that allocates the

functionality of traditional edge routers (as well as additional functionality) among three logical modules: a programmable access device, an external processor, and an access router. Basic routing of packets between input and output ports of the access network is performed by the access router. However, forwarding and generic traffic conditioning functions, such as marking, policing, monitoring, shaping, and filtering, are implemented in the programmable access device (*see, e.g.,* independent claim 50), and service functions, such as message interpretation, signaling, admission control, and policy invocation, are implemented in the external processor (*see, e.g.,* independent claims 1 and 26). (*See, e.g.,* specification, p. 5, lines 3 - 32)

More specifically, for example, a communication network 30 includes one or more core communication links 38 (e.g., trunk lines) coupled to one or more core routers 36. However, in contrast to conventional communication networks, such as that illustrated in Figure 1, customer router 32 does not interface to communication network 30 via a monolithic, proprietary edge router. Instead, customer equipment, such as customer router 32, interfaces with communication 30 via a network access system 31 that distributes the functions of traditional edge routers (as well as additional functionality) among three logical modules: a programmable access device (PAD) 40, an external processor 42, and an access router 44. Basic routing of packets between input and output ports of the access network is performed by access router 44 by reference to forwarding table 50 as determined by Exterior Gateway Protocol (EGP) and Interior Gateway Protocol (IGP) routing tables 52 and 54. However, forwarding and generic traffic conditioning functions, such as marking, policing, monitoring, shaping, and filtering, are implemented in programmable access device 40 (*see, e.g.,* independent claim 50), and service functions, such as message interpretation, signaling, admission control, and policy invocation, are implemented in external processor 42 (*see, e.g.,* independent claims 1 and 26). Given this distribution of

functionality, incoming and outgoing packets are typically communicated between core communication links 38 and customer router 32 via programmable access device 40, access router 44, and core router 36 (and optionally additional switching the access network, such as an Asynchronous Transfer Mode (ATM) or Multiprotocol Label Switching (MPLS) switch 60).

If filtering functionality of the programmable access device (PAD) 40 detects packet flows for which services, additional to typical services afforded by the configuration to incoming and outgoing packets are appropriate, the programmable access device 40 passes appropriate messages to the external processor 42 (*See, e.g.,* independent claims 1 and 26) for service processing via a Message, Control, and Reporting Interface (MCRI) 58 (*See, e.g.,* independent claim 50), which can be accessed via an Application Programming Interface (API) on the programmable access device 40 and external processor 42. Distributing functionality between access router 44, programmable access device 40 and external processor 42 in this manner gives the service provider (or even third parties) the freedom to extend and modify existing services, create new services, or add more processing power to external processor 42 without adversely affecting the forwarding performance of the programmable access device 40 and the routing performance or functionality of access router 44. This distribution of functionality results in numerous advantages, including improved scalability, flexibility, extensibility, interoperability, security, and service provisioning.

To implement a desired functionality for programmable access device 40 and external processor 42, the service provider (or even a customer or third party) can define policy rules in the policy database 46 of one or more servers 48 (also referred to as a policy decision point (PDP)). Policy server 48 then makes policy decisions that control the functionality and operation of programmable access device 40 and external processors 42 by reference to the policy rules

stored in policy database 46. Policy server 48 communicates policy decisions and associated configuration parameters for external processor 42 via a Service Policy Interface (SPI) 56, which can be accessed, for example, via an application program interface (API) on policy server 48 and external processor 42. Communication via Service Policy Interface 56 can employ any of a number of policy query protocols, including Common Open Policy Service (COPS) and Lightweight Directory Access Protocol (LDAP), which are respectively defined by Internet Engineering Task Force (IETF) RFCs 2748 and 2251. External processor 42 relays configuration parameters for programmable access device 40, if any, to programmable access device 40 via Message, Control, and Reporting Interface 58. (*See, e.g.,* specification, p. 10, line 14 - p. 11, line 31, FIGs. 2, 4)

Generally speaking, the functional modules of programmable access device 40 are logically arranged in incoming (e.g., from customer router 32) and outgoing (e.g., to customer router 32) traffic paths, with the incoming path including packet header filter 80, marker/policer 82, monitor(s) 84, forwarding table 86, and output buffers and scheduler 88. The outgoing path similarly includes packet header filter 90, forwarding table 86, monitor(s) 92, marker/shaper 94, and output buffers and scheduler 96. The functions of all of these functional modules can be independently configured or programmed by an external processor 42 through Message, Control, and Reporting Interface 58. (*See, e.g.,* independent claims 1, 26, and 50)

Incoming packets received from customer router 34 at the external interface of programmable access device 40 are first processed by packet header filter 80, which distinguishes between various message types using any one or a combination of the protocol type, Source Address (SA), Destination Address (DA), Type Of Service (TOS), Diffserv Codepoint (DSCP), Source Port (SP), Destination Port (DP), and other fields of a packet (e.g., layer 4 and higher

layer fields such as the SYN, ACK, RST, and FIN TCP flags) upon which packet header filter 80 is configured to filter. In addition to filtering on layer-3 information, packet header filter 80 has the ability to identify higher layer (i.e., layer 4-7) message types or specific fields and forward those messages from/to external processor 42 based on the configured filter parameters. Thus, based upon its filter configuration and the fields of an incoming packet, packet header filter 80 directs the packet either to an external processor 42 via message interface 100 or to a specific marker/policer 82 (*see,* e.g., independent claims 1, 26, and 50). Message interface 100 may also inject a packet specified by external processor 42 into either of packet header filters 80 and 90. (*See, e.g.,* specification, p. 13, lines 7-32, FIGs. 2, 3)

In response to a stream of packets from packet header filter 80, marker/policer 82 polices the packet stream by applying one or more token or leaky bucket algorithms to determine whether the packet stream conforms to the traffic parameters established by control interface 104. As a result of the policing function, marker/policer 82 may discard nonconforming packets, mark nonconforming packets (e.g., with a higher or lower priority), and/or count nonconforming packets, depending upon its configuration (*See,* e.g., independent claim 50). If marking is required, marker/policer 82 may set bits in the Differentiated Services (DiffServ)/TOS byte in the IP packet header, and/or the 3-bit Multiprotocol Label Switching (MPLS) experimental field, and/or the 20-bit MPLS label field, and/or other fields as configured by control interface 104 for that particular packet stream.

Within the incoming path, one or more monitors 84 having different functions may be included. For example, these monitors 84 may include a usage monitor that tracks statistics for different layer-2, layer-3, layer-4, and higher layer traffic types (e.g., to monitor a Service Level Agreement (SLA)). Monitors 84 may also include a fault/troubleshooting/debugging monitor

(*see, e.g.,* dependent claim 11) that verifies conformance to standards to standards and assists in code debugging and fault diagnosis by saving and reporting memory dumps and other related information to external processor 42 via reporting interface 102 and Message, Control, and Reporting Interface 58. To regulate reporting messages, thresholds and other criteria can be set up to invoke a reporting event. The reporting messages sent to external processor 42 by monitors 84 may summarize usage information for a particular customer, report the occurrence of a high-priority traffic flow, alert external processor 42 to a large volume of out-of-band traffic, report on inactivity of a monitored flow, etc.

After processing by packet header filter 80, incoming packets are processed by forwarding table 86 (*see, e.g.,* independent claims 1 and 26). Forwarding table 86 maintains entries for each forwarding path, where each forwarding path is represented by packet flow attributes, such as DA, SA, TOS, PT, SP, DP, the incoming port, and the corresponding output port to which programmable access device 40 forwards the packet through the access network toward access router 44. Utilizing these forwarding table entries, forwarding table 86 forwards packets to the appropriate output ports and passes the packets to output buffers and scheduler 88. Output buffers and scheduler 88 buffer packets ready for transmission over communication network 30 and schedule the transmission of such packets. (*See, e.g.,* specification, page 14, line 1 - page 15, line 9, FIGs. 2, 3)

The outgoing path through programmable access device 40 is similar to the incoming path, except for the inclusion of marker/shaper 94 in lieu of marker/policer 82 (*see,* e.g., independent claim 50). Marker/shaper 94 discards nonconforming packets, sends marked packets to appropriate output buffers for the various queues serving different QoS classes for individual flows within output buffers and scheduler 96 to control the delay, jitter and loss of an outgoing

packet flow, or simply counts non-conforming packets. (*See, e.g.*, specification, page 15, lines 24-30, FIGs. 2, 3)

The external processor 42 performs at least three types of processing: invoking policy services, signaling to setup and teardown access network connections, and configuring one or more associated programmable access devices 40. To coordinate these different processing functions, external processor 42 contains one or more service controllers 120, which each may control these three functions for a respective type of service. For example, service controllers 120 may include any or all of a Conference Call Service Controller (CCSC), an E-Commerce Service Controller (ECSC), an IP Telephony Service Controller (IPTELSC), a Reserved Bandwidth Service Controller (RBSC), and a Multicast Service Controller (MSC). Each service controller may maintain a session table recording all of its active sessions with a programmable access device 40.

As further shown in FIG. 4, external processor 42 includes, for each associated programmable access device 40, a respective programmable access device controller 124. Under the direction of service controller(s) 120, each programmable access device controller 124 configures forwarding table 86, packet header filters 80 and 90, marker/policer 82, marker/shaper 94, monitors 84 and 92, and output buffers and schedulers 88 and 96 of the associated programmable access device 40 by invoking commands or scripts understood by control interface 104. External processor 42 also contains a respective message processor 122 for each associated programmable access device 40. Message processors 122 each communicate messages to and from the message interface 100 of the associated programmable access device 40. Upon receipt of a message from a programmable access device 40, which is usually a message received from the customer router 32, a message processor 122 parses the message and informs the appropriate

service controller (as determined by the type of service) of its contents. (*See, e.g.,* specification, page 17, lines 4-31, FIGs. 3, 4)

Upon receipt of a report message from a reporting processor 126 or another message type from a message processor 122 included in the external processor 42, a service controller 120 of the external processor translates the message into one or more policy queries and transmits the policy query or queries to a policy server 48 via a Service Policy Interface (SPI) 56. A service controller 120 may also pass a message to another service controller 120 to obtain additional services via an interface 121.

In response to receipt of a policy decision from policy server 48, service controller 120 may inject one or more packets into a traffic flow via message processor 122, configure a programmable access device 40 via programmable access device controller 124 or control signaling inside or outside communication network 30 via signaling controllers 128a and 128b. Signaling controllers 128 support signaling protocols (e.g., Resource ReSerVation Protocol RSVP, Label Distribution Protocol (LDP), Private Network-Network Interface (PNNI), frame relay or ATM User Network Interface (UNI), etc.) to setup or tear down a Virtual Connection (VC) or Label Switched Path (LSP) across the network. A VC or LSP setup by a signaling controller 128 may have a specified Quality of Service (QoS). (*See, e.g.,* specification, page 18, lines 13-31, FIGs. 2, 4, *see, also, e.g.,* specification, p. 29, line 20 - p. 30, line 27)

In summary, a distributed network access system consistent with features of the present invention replaces a monolithic edge router with a programmable access device containing at least filtering and forwarding functionality, an external processor having one or more service-specific controllers that implement policy-based control of the programmable access device, and an access router that performs basic routing. This distributed architecture has numerous benefits

over conventional monolithic router architectures, including scalability flexibility, extensibility, interoperability, security, and service provisioning. (*See, e.g.*, specification, page 49, line 29 - page 50, line 5)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-5, 15, 17, 21-22, 26-30, 39, 41, and 45-46 are obvious under 35 U.S.C. § 103(a) based on *Amara et al.* (U.S. 6,674,743) in view of *Bhattacharya et al.* (U.S. 6,587,466).

Whether claims 6-10, 12-14, 16, 18, 23-25, 31-35, 37-38, 40, 42, and 47-50 are obvious under 35 U.S.C. § 103(a) based on *Amara et al.* and *Bhattacharya et al.* and further in view of *Gai et al.* (U.S. 6,167,445).

Whether claims 19 and 43 are obvious under 35 U.S.C. § 103(a) based on *Amara et al.* and *Bhattacharya et al.* and further in view of *Gibson et al.* (U.S. 6,680,943).

Whether claims 20 and 44 are obvious under 35 U.S.C. § 103(a) based on *Amara et al.* and *Bhattacharya et al.* and further in view of *Jorgensen* (U.S. 6,452,915).

Whether claims 11 and 36 are obvious under 35 U.S.C. § 103(a) based on *Amara et al.*, *Bhattacharya et al.*, and *Gai et al.* and further in view of *Natarajan et al.* (U.S. 6,505,244).

VII. ARGUMENT

A. CLAIMS 1-50 ARE NOT RENDERED OBVIOUS BY *AMARA ET AL., BHATTACHARYA ET AL., GAI ET AL., GIBSON ET AL., JORGENSEN, AND NATARAJAN ET AL.*

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention under any statutory provision always rests upon the Examiner. *In re Mayne*, 104 F.3d 1339, 41 USPQ2d 1451 (Fed .Cir. 1997); *In re Deuel*, 51 F.3d 1552, 34 USPQ2d 1210 (Fed. Cir. 1995); *In re Bell*, 991 F.2d 781, 26 USPQ2d 1529 (Fed. Cir. 1993); *In re Oetiker*, 977 F.2d 1443,

24 USPQ2d 1443 (Fed. Cir. 1992). In rejecting a claim under 35 U.S.C. § 103, the Examiner is required to provide a factual basis to support the obviousness conclusion. *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967); *In re Lunsford*, 357 F.2d 385, 148 USPQ 721 (CCPA 1966); *In re Freed*, 425 F.2d 785, 165 USPQ 570 (CCPA 1970).

Obviousness rejections require some evidence in the prior art of a teaching, motivation, or suggestion to combine and modify the prior art references. See, e.g., *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1351-52, 60 USPQ2d 1001, 1008 (Fed. Cir. 2001); *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25, 56 USPQ2d 1456, 1459 (Fed. Cir. 2000); *In re Dembiczak*, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

The rejection of claims 1-50 must be reversed because the references at least do not disclose "passes identified messages via a message interface to an external processor included in said network access system for implementation of the policy-based services by the external processor, wherein said packet header filter passes all other received messages through the packet header filter to an other processor" as recited by independent claim 1, "passing identified messages to an external processor included in the network access system for implementation of the policy-based services by the external processor" and "for messages that are not identified, routing packets by reference to a forwarding table in the programmable access device and outputting the routed packets at a second network interface of the programmable access device" as recited by independent claim 26, or "a message interface coupled to an external processor that is configured to implement policy-based services" and "the second packet header filter identifies messages, received from the second network interface, on which policy-based services are to be implemented, wherein the second packet header filter passes the identified

messages to the external processor via the message interface and passes all other messages received from the second network interface to the marker" as recited by independent claim 50.

Amara et al. is directed to applying policies in packet forwarding devices, such as routers and remote access servers. (Col. 1: 9-11) *Amara et al.* (per col. 2: 58-67) recognizes a problem with certain systems of a high overhead associated with applying policies to all incoming and outgoing packets, increasing the latency of each packet, and disadvantageously requiring time and effort to develop and manage policies for each interface. *Amara et al.* (per col. 3: 2-11) includes an internal application that generates internally-generated packets. A policy is applied to the internally-generated packets, and the packets are then forwarded to a first interface. External packets are received at a second interface, and the external packets are forwarded to the first interface without applying the policy to them.

Additionally, at col. 6: 9-25, *Amara et al.* states:

> Policy engine 232 applies a policy to the internal packets, i.e., the internally-generated packets generated by internal applications 230 and the internally-destined packets used by internal applications 230. Policy engines 224-228 apply policies to the external packets forwarded by packet classifiers 214-218, respectively. Policy engines 224-228 typically also apply policies to the external packets forwarded by packet forwarder 222.
>
> In this way, device 200 applies policies to the internal packets and to the external packets. In general, the policies applied to the internal and external packets may differ. The approach used in device 200 may not realize the efficiency advantage afforded by the approach used in device 100. However, by applying policies to internal packets using policy engine 232, regardless of which of interfaces 202-206 may transmit or receive the packet, the task of policy management is greatly simplified.

1. CLAIMS 1-5, 15, 17, 21-22, 26-30, 39, 41, AND 45-46 ARE NOT RENDERED OBVIOUS BY *AMARA ET AL.* IN VIEW OF *BHATTACHARYA ET AL.*

Regarding claims 1 and 26, the Examiner (Office Action dated November 18, 2004, pp. 2-3) correctly acknowledges that *Amara et al.* "does not explicitly indicate that said packet

header filter identifies messages received at to [*sic*] one of the first and second network interfaces on which policy-based services are to be implemented and passes identified messages via a message interface to an external processor <u>included in said network access system</u> for <u>implementation of the policy-based services by the external, [*sic*] wherein said packet header filter passes all other received messages through the packet header filter to another processor</u>" and then relies on *Bhattacharya et al.* for these features.

Bhattacharya et al. (per Abstract) is directed to constructing and using a search tree structure to accomplish policy based service differentiation in packet networks by reducing the number of steps performed to implement packet classification. *Bhattacharya et al.* uses a method of preprocessing a given set of policy rules by modeling the conditions in the rules as multidimensional hyper-cubes to construct a search tree. Using the search tree, packet classification is achieved by determining all applicable policies with compare and branch instructions.

As best understood, the Examiner (Office Action dated November 18, 2004, p. 3), citing col. 5: 50-60 and col. 12: 8-14 of *Bhattacharya et al.*, equates the recited "programmable access device" with the Policy Enforcement Entity **240** of *Bhattacharya et al.* and equates the recited "external processor" with the Combined Policy Matching Engine **220**, and then contends that *Bhattacharya et al.* discloses "messages received on which policy-based services are to be implemented and passes identified messages via a message interface to an external processor <u>included in said network access system</u> for <u>implementation of the policy-based services by the external (Column 6, lines 44-50), [*sic*] wherein said packet header filter passes all other received messages through the packet header filter to another processor (Column 6, lines 50-56)</u>."

Further, in the Advisory Action dated March 15, 2005, the Examiner contends:

> The applicant argues that the combination of Amara in view of Bhattacharya does not indicate that the device sends selected messages to an external processors [*sic*] that need policy implemented on those packets. The examiner disagrees because the reference, Bhattacharya discloses identifying messages that need policy applied to them and sending the identified information through a message interface to an external processor/polcy [*sic*] implementer to help implemente [*sic*] the correct policy on that message.

However, at col. 12: 8-14, *Bhattacharya et al.* states:

> Alternatively, the **Combined Policy-matching Engine** may be located in an external policy server and **policy decisions may be outsourced to this device**, while the **service specific modules are located at the Policy Enforcement Entity** such as the router or firewall. In such an architecture, the policy server functions as a single **policy decision** point serving a number of different network devices.

At col. 6: 13-23, *Bhattacharya et al.* states:

> In this architecture, the Policy Enforcement Entity 240 obtains all actions that are applicable for a packet by querying the Combined Policy-matching Engine 220. The **decisions returned** by the Combined Policy-matching Engine 220 determine the **actual treatment that a packet receives within the Policy Enforcement Entity 240**. It may also influence the order in which the service specific modules, such as Security Enforcement Module 280 and QOS Enforcement Module 290, process the entering packets 240 before they leave the device in a possibly conditioned or transformed state 245.

Further, the decisions **270** returned by the Combined Policy-matching Engine **220** of *Bhattacharya et al.* depend on the "set of values for Selectors 260 which are defined as the attributes associated with an incoming packet that are necessary for packet classification. Policy Enforcement Entity 240 **provides these values as inputs in the query** using the Combined Policy-matching Engine Interface 250." (Col. 6: 24-33)

Thus, any "implementation of the policy-based services" is, at best, performed by the Policy Enforcement Entity **240**, and is **not** performed by the Combined Policy-matching Engine **220**. Furthermore, there are no received "messages" that are identified as "messages on which

policy-based services are to be implemented" and which are **passed** to the Combined Policy-matching Engine **220** by any "packet header filter," as *Bhattacharya et al.*'s Policy Enforcement Entity **240** (per FIG. 2) sends **queries with selectors** or CPE state updates **260** to the Combined Policy-matching Engine **220** to receive a decision **270** in response. Therefore, "implementation of the policy-based services by the external processor" as recited by independent claims 1 and 26 is not suggested or disclosed by *Bhattacharya et al.*, singly nor in any reasonable combination with *Amara et al.*

Furthermore, since there are no "messages" passed by any "packet header filter", there are also no "other received messages" to be passed "to another processor" (e.g., as recited by claim 1) or "messages that are not identified" to be routed "to a forwarding table." (e.g., as recited by claim 26), and the Examiner fails to explain how these features are met by the references.

Appellants assert that the reasoning that the Examiner puts forth for the rejection at least with respect to "other received messages" and "messages that are not identified" contravenes 35 U.S.C. § 132, which requires the Director to "notify the applicant thereof, stating the reasons for such rejection." This section is violated if the rejection "is so uninformative that it prevents the applicant from recognizing and seeking to counter the grounds for rejection." *Chester v. Miller*, 906 F.2d 1574, 15 USPQ2d 1333 (Fed. Cir. 1990). This policy is captured in the Manual of Patent Examining Procedure. For example, MPEP § 706 states that "[t]he goal of examination is to clearly articulate any rejection early in the prosecution process so that applicant has the opportunity to provide evidence of patentability and otherwise respond completely at the earliest opportunity." Furthermore, MPEP § 706.02(j) indicates that: "[i]t is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the applicant can be given fair opportunity to reply."

Therefore, the rejection of claims 1 and 26 should be withdrawn.

The rejection of dependent claims 2-5, 15, 17, 21-22, 27-30, 39, 41, and 45-46 should be withdrawn for at least the same reasons as their respective independent claims, and these claims are separately patentable on their own merits.

2. CLAIMS 6-10, 12-14, 16, 18, 23-25, 31-35, 37-38, 40, 42, and 47-50 ARE NOT RENDERED OBVIOUS BY *AMARA ET AL. AND BHATTACHARYA ET AL. AND FURTHER IN VIEW OF GAI ET AL.*

Regarding the rejection of independent claim 50, the recited features are neither suggested nor disclosed by any reasonable combination of *Amara et al.*, *Bhattacharya et al.*, and *Gai et al.*, and the Examiner fails to explain how the recited features are suggested or disclosed by these references. For example, in the Office Action dated November 18, 2004, p. 9, the Examiner states, "Amara also does not explicitly indicate that **the policer comprises a marker** that marks packets that do not conform with the traffic parameters. Gai teaches a method of identifying packets which do not conform with the traffic parameters and a way to mark those packets (Column 20, lines 2-9; Column 4, line 64 - Column 5, line 8) and discarding those packets (Column 20, lines 2-9)."

Appellants respectfully submit that the Examiner does not track the recited language of claim 50, for example, with regard to the "policer" and the "marker," for which claim 50 recites, "a policer configured to discard packets determined as nonconforming to a first traffic parameter," "a marker configured to discard packets determined as nonconforming to a second traffic parameter," "a message interface coupled to an external processor that is configured to implement policy-based services" and "the second packet header filter identifies messages, received from the second network interface, on which policy-based services are to be implemented, wherein the second packet header filter **passes the identified messages to the**

external processor via the message interface and passes all other messages received from the second network interface to the marker," and the Examiner does not explain how these features are met by the references. However, for reasons similar to those discussed previously, Applicants respectfully submit that these features are not suggested or disclosed by *Amara et al.* and *Bhattacharya et al.*, and the addition of *Gai et al.* does not fill in the gaps.

Gai et al. (per Abstract) is directed to translating high-level network policies, in networks having multiple, dissimilar network devices, into a set of rules that can be put into effect by specific network devices.

In the Advisory Action dated March 15, 2005, the Examiner contends:

> Regarding the applicant's argument for claim 50, that the combination of the references, Amara, Bhattacharya, and Gai does not meet the limitations. The examiner disagrees, the reference Amara discloses a first and second header filter, which identifies messages, but does not explicitly indicate that those filter [*sic*] can mark or drop packets. Gai discloses a system which identifies packets, and which discards, marks, or marks and discards packets based on the identification and a policy of diferring [*sic*] traffic parameteres [*sic*]. The combination of Gai and Amara discloses that Amara's system can be improved using Gai's teaching of double checking many traffic parameter's [*sic*] and marking/discarding packets based on those traffic parameters.

However, this argument continues to ignore "the second packet header filter **passes the identified messages to the external processor via the message interface and passes all other messages received from the second network interface to the marker**" as clearly recited by claim 50, as pointed out above. Moreover, Appellants assert that the reasoning that the Examiner puts forth for the rejection at least with respect to "the second packet header filter **passes the identified messages to the external processor via the message interface and passes all other messages received from the second network interface to the marker**" contravenes 35 U.S.C. § 132, MPEP § 706, and *Chester v. Miller*, *supra*. As discussed

previously, "[i]t is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the applicant can be given fair opportunity to reply." The Examiner has failed in this regard.

Therefore, the rejection of claim 50 should be reversed.

Furthermore, with regard to the rejection of dependent claims 6-10, 12-14, 16, 18, 23-25, 31-35, 37-38, 40, 42, and 47-49, Appellants respectfully submit that the deficiencies of *Amara et al.* and *Bhattacharya et al.* discussed previously are not cured by the secondary reference of *Gai et al.*, which is cited by the Examiner for a supposed teaching of a way to identify and mark packets that do not conform with traffic parameters, as teaching monitoring traffic entering a device, issuing thresholds for priority queuing and traffic classes, a plurality of output buffers, a scheduler, the use of user priority, and a reporting interface. (Office Action dated November 18, 2004, pp. 4-9) Thus, the rejection of claims 6-10, 12-14, 16, 18, 23-25, 31-35, 37-38, 40, 42, and 47-49 should also be reversed.

3. CLAIMS 19 AND 43 ARE NOT RENDERED OBVIOUS BY *AMARA ET AL. AND BHATTACHARYA ET AL. AND FURTHER IN VIEW OF GIBSON ET AL.*

Claim 19 recites, "wherein the identified message is a session initiation protocol (SIP) message." *Gibson et al.*, directed (per Abstract) to a establishing a path for a communication session over a communications network, is cited by the Examiner as supposedly teaching the use of Session Initiation Protocol (SIP) messages. (Office Action dated November 18, 2004, p. 9)

Gibson et al. similarly fails to cure the deficiencies of *Amara et al.*, *Bhattacharya et al.*, and *Gai et al.* as discussed previously, and thus the rejection of claims 19 and 43 should be reversed.

4. CLAIMS 20 AND 44 ARE NOT RENDERED OBVIOUS BY *AMARA ET AL. AND BHATTACHARYA ET AL. AND FURTHER IN VIEW OF JORGENSEN.*

Claim 20 recites, "wherein the identified message is an Internet Group Multicast Protocol (IGMP) message." *Jorgensen*, directed (per Abstract) to an IP flow classification system used in a wireless telecommunications system, is cited by the Examiner as supposedly teaching the use of Internet Group Multicast Protocol messages. (Office Action dated November 18, 2004, p. 10)

Jorgensen similarly fails to cure the deficiencies of *Amara et al.*, *Bhattacharya et al.*, *Gai et al.*, and *Gibson et al.* as discussed previously, and thus the rejection of claims 20 and 44 should be reversed.

5. CLAIMS 11 AND 36 ARE NOT RENDERED OBVIOUS BY *AMARA ET AL., BHATTACHARYA ET AL., GAI ET AL., AND FURTHER IN VIEW OF NATARAJAN ET AL.*

Claim 11 recites the "programmable access device of Claim 7, and further comprising a fault monitor." *Natarajan et al.* is cited by the Examiner as supposedly teaching the use of a fault monitor in a policy system in a network node. (Office Action dated November 18, 2004, p. 10) However, *Natarajan et al.* is directed (per Abstract) to a feedback-based adaptive network wherein at least a portion of the network elements report operating information relating to network conditions to a centralized data store. The information which is reported to the data store is analyzed by a policy engine which includes a plurality of application specific plug-in policies for analyzing specific information from the data store and for computing updated control information based upon the analysis of the information. The updated control information is then fed back to selected network elements to thereby affect operation of the selected elements.

Natarajan et al. also fails to cure the deficiencies of *Amara et al.*, *Bhattacharya et al.*, *Gai et al.*, *Gibson et al.*, and *Jorgensen* as discussed previously, and thus the rejection of claims 20 and 44 should be reversed.

Thus, Appellants respectfully request reversal of the rejections with respect to claims 1-50.

VIII. CONCLUSION AND PRAYER FOR RELIEF

For the foregoing reasons, Appellants request the Honorable Board to reverse each of the Examiner's rejections.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

6/15/05
Date

Reg. No. 44,658
Margo Livesay, Ph.D.
Attorney for Applicant(s)
Reg. No. 41,946

10507 Braddock Rd, Suite A
Fairfax, VA 22032
Tel. 703-425-8508
Fax. 703-425-8518

CLAIMS APPENDIX

1. (Previously Presented) A programmable access device for use in a network access system, said programmable access device comprising:

first and second network interfaces through which packets are communicated with a network;

a packet header filter and a forwarding table, wherein the forwarding table is utilized to forward packets between the first and second network interfaces, and wherein said packet header filter identifies messages received at one of the first and second network interfaces on which policy-based services are to be implemented and passes identified messages via a message interface to an external processor included in said network access system for implementation of the policy-based services by the external processor, wherein said packet header filter passes all other received messages through the packet header filter to an other processor.

2. (Original) The programmable access device of Claim 1, wherein the packet header filter receives packets directly from the first network interface.

3. (Original) The programmable access device of Claim 2, wherein the packet header filter is a first packet header filter, and wherein the programmable access device further comprises a second packet header filter that receives packets directly from the second network interface.

4. (Original) The programmable access device of Claim 1, wherein the packet header filter filters packets for service processing based upon protocol information pertaining to protocol layers higher than layer 3.

5. (Original) The programmable access device of Claim 1, and further comprising a policer that polices packets by reference to traffic parameters.

6. (Original) The programmable access device of Claim 5, wherein the policer comprises a marker that marks packets that do not conform with the traffic parameters.

7. (Original) The programmable access device of Claim 1, and further comprising at least a usage monitor that monitors at least one traffic type.

8. (Original) The programmable access device of Claim 7, wherein the usage monitor has an associated threshold that when exceeded generates a reporting event for the usage monitor.

9. (Previously Presented) The programmable access device of Claim 8, and further comprising a reporting interface that communicates the reporting event to the external processor.

10. (Original) The programmable access device of Claim 9, wherein the associated threshold comprises a session activity level threshold.

11. (Original) The programmable access device of Claim 7, and further comprising a fault monitor.

12. (Original) The programmable access device of Claim 1, and further comprising one or more output buffers for outgoing packets.

13. (Original) The programmable access device of Claim 12, and further comprising a scheduler associated with the one or more output buffers that schedules the transmission of outgoing packets within the one or more output buffers.

14. (Original) The programmable access device of Claim 13, wherein the scheduler supports multiple quality of service classes.

15. (Original) The programmable access device of Claim 1, and further comprising a control interface through which said packet header filter and said forwarding table are programmed.

16. (Original) The programmable access device of Claim 15, and further comprising at least a programmable monitor that monitors at least one programmed traffic type.

17. (Original) The programmable access device of Claim 15, and further comprising a policer that polices packets by reference to programmed traffic parameters.

18. (Original) The programmable access device of Claim 15, and further comprising one or more output buffers for outgoing packets and an associated scheduler that transmits the outgoing packets from the one or more output buffers through the second network interface according to a programmed methodology.

19. (Original) The programmable access device of Claim 1, wherein the identified message is a session initiation protocol (SIP) message.

20. (Original) The programmable access device of Claim 1, wherein the identified message is an Internet Group Multicast Protocol (IGMP) message.

21. (Original) The programmable access device of Claim 1, wherein the identified message is a Resource Reservation Protocol (RSVP) message.

22. (Original) The programmable access device of Claim 1, and further comprising a plurality of protocol-specific state machines for a respective plurality of protocol types.

23. (Previously Presented) The programmable access device of Claim 22, wherein said plurality of protocol-specific state machines include a transport control protocol (TCP) state machine that, responsive to a control command, provides preferential treatment to a particular TCP session.

24. (Previously Presented) The programmable access device of Claim 1, and further comprising a reporting interface through which the programmable access device reports state information for active sessions to the external processor.

25. (Original) The programmable access device of Claim 24, wherein the reporting interface reports the state information for an active session in response to allocation of service to a new external service controller.

26. (Previously Presented) A method of packet handling in a programmable access device of a network access system, said method comprising:

in response to receiving a series of packets at a first network interface of a programmable access device, filtering the series of packets at the programmable access device to identify messages upon which policy-based services are to be implemented;

passing identified messages to an external processor included in the network access system for implementation of the policy-based services by the external processor;

and

for messages that are not identified, routing packets by reference to a forwarding table in the programmable access device and outputting the routed packets at a second network interface of the programmable access device.

27. (Previously Presented) The method of Claim 26, and further comprising receiving packets at the packet header filter directly from the first network interface.

28. (Original) The method of Claim 27, wherein the packet header filter is a first packet header filter, said method further comprising receiving packets at a second packet header filter of the programmable access device directly from the second network interface.

29. (Original) The method of Claim 26, wherein filtering comprises filtering packets for service processing based upon protocol information pertaining to protocol layers higher than layer 3.

30. (Original) The method of Claim 26, and further comprising policing packets by reference to traffic parameters utilizing a policer in the programmable access device.

31. (Original) The method of Claim 30, wherein policing comprises marking packets that do not conform with the traffic parameters.

32. (Previously Presented) The method of Claim 26, wherein the programmable access device includes at least a usage monitor, said method further comprising monitoring at least one traffic type in said series of packets.

33. (Original) The method of Claim 32, wherein the usage monitor has an associated threshold, said method further comprising generating a reporting event for the usage monitor when the threshold is exceeded.

34. (Original) The method of Claim 33, and further comprising communicating the reporting event to an external processor via a reporting interface.

35. (Original) The method of Claim 34, wherein generating a reporting event comprises generating a reporting event in response to a session activity level threshold.

36. (Original) The method of Claim 32, and further comprising monitoring faults utilizing a fault monitor in said programmable access device.

37. (Original) The method of Claim 26, and further comprising buffering outgoing packets in one or more output buffers in said programmable access device.

38. (Original) The method of Claim 37, and further comprising scheduling the transmission of outgoing packets within the one or more output buffers to support multiple quality of service classes.

39. (Original) The method of Claim 26, and further comprising programming said programmable access device through a control interface of said programmable access device.

40. (Original) The method of Claim 39, wherein the programmable access device further includes at least one programmable monitor, said method further comprising monitoring at least one programmed traffic type utilizing said at least one programmable monitor.

41. (Original) The method of Claim 39, wherein said programmable access device includes a policer, said method further comprising policing packets by reference to programmed traffic parameters.

42. (Original) The method of Claim 39, wherein the programmable access device includes one or more output buffers for outgoing packets and an associated scheduler, said method comprising transmitting the outgoing packets from the one or more output buffers through the second network interface according to a programmed methodology.

43. (Original) The method of Claim 26, wherein the identified message is a session initiation protocol (SIP) message.

44. (Original) The method of Claim 26, wherein the identified message is an Internet Group Multicast Protocol (IGMP) message.

45. (Original) The method of Claim 26, wherein the identified message is a Resource Reservation Protocol (RSVP) message.

46. (Original) The method of Claim 26, and further comprising maintaining in said programmable access device a plurality of protocol-specific state machines for a respective plurality of protocol types.

47. (Original) The method of Claim 26, wherein said plurality of protocol-specific state machines include a transport control protocol (TCP) state machine, and wherein the method further comprises providing preferential treatment to a particular TCP session by said programmable access device in response to a command.

48. (Original) The method of Claim 26, and further comprising reporting state information for active sessions to an external processor via a reporting interface of the programmable access device.

49. (Original) The method of Claim 48, wherein reporting comprises reporting the state information for an active session in response to allocation of service to a new external service controller.

50. (Previously Presented) A device for use in a network access system comprising:

a first network interface through which packets are communicated with a first network;

a second network interface through which packets are communicated with a second network;

a message interface coupled to an external processor that is configured to implement policy-based services;

a policer configured to discard packets determined as nonconforming to a first traffic parameter;

a first packet header filter coupled to the first network interface and to the message interface, wherein the first packet header filter identifies messages, received from the first

network interface, on which policy-based services are to be implemented, wherein the first packet header filter passes the identified messages to the external processor via the message interface and passes all other messages received from the first network interface to the policer;

a marker configured to discard packets determined as nonconforming to a second traffic parameter; and

a second packet header filter, different from the first packet header filter, coupled to the second network interface, wherein the second packet header filter identifies messages, received from the second network interface, on which policy-based services are to be implemented, wherein the second packet header filter passes the identified messages to the external processor via the message interface and passes all other messages received from the second network interface to the marker.